Homework 7

Mark Schulist

1)

1.a)

1.a.i)

$$\begin{aligned}\log_2(8) &= a \\ 2^a &= 8 \bmod 11 \\ a &= 3\end{aligned}\tag{1}$$

1.a.ii)

$$\begin{aligned}\log_6(3) &= a \\ 6^a &= 3 \bmod 11 \\ a &= 2\end{aligned}\tag{2}$$

1.a.iii)

$$\begin{aligned}\log_6(3) &= a \\ 6^a &= 3 \bmod 13 \\ a &= 8\end{aligned}\tag{3}$$

1.b)

1.b.i)

$$x^7 = 8 \bmod 11\tag{4}$$

2 is a primitive root mod 11. Let $g = 2$. We know that $\log_2(8) = 3$, so let $x = 2^k$.

$$\begin{aligned}\left(2^k\right)^7 &= 2^3 \bmod 11 \\ 7k &= 3 \bmod 10 \\ k &= 9 \bmod 10\end{aligned}\tag{5}$$

So $x = 2^9 = 6 \bmod 11$.

1.b.ii)

$$x^4 = 3 \bmod 11\tag{6}$$

We know that $\log_6(3) = 2$, and let $x = 6^k$.

$$\begin{aligned}\left(6^k\right)^4 &= 6^2 \bmod 11 \\ 4k &= 2 \bmod 10 \\ k &= 3, 8\end{aligned}\tag{7}$$

So $x = 6^3 = 7 \bmod 11$ and and $x = 6^8 = 4 \bmod 11$ are solutions.

1.b.iii)

$$x^3 = 3 \bmod 13 \tag{8}$$

We know $\log_6(3) = 8$. Let $x = 6^k$.

$$\begin{aligned}\left(6^k\right)^3 &= 6^8 \bmod 13 \\ 3k &= 8 \bmod 12\end{aligned} \tag{9}$$

There are no solutions, so there are no solutions to $x^3 = 3 \bmod 13$.

2)

$g \in (\mathbb{Z}/p\mathbb{Z})^\times$, g primitive root.

Suppose $\log_g(b)$ is computable for $b \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Show we can now solve $a^x = b \bmod p$ for any $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Let $a = g^k$ for some $k \in \mathbb{Z}$.

Then

$$\begin{aligned}\left(g^k\right)^x &= b \bmod p \\ g^{kx} &= b \bmod p\end{aligned} \tag{10}$$

Compute $\log_g(b) = d$.

$$\begin{aligned}kx &= \log_g(b) \bmod p - 1 \\ kx &= d \bmod p - 1 \\ k^{-1}kx &= dk^{-1} \bmod p - 1 \\ x &= dk^{-1} \bmod p - 1\end{aligned} \tag{11}$$

3)

$p = 1373, g = 2, A = 974, b = 871$

$$B = 2^{871} = 805 \tag{12}$$

$$B' = A^b = 974^{871} = 397 \tag{13}$$

So the shared secret is 397.

4)

4.a)

$m = 583, B = 469, k = 877.$

$c_1 = g^k = 719, c_2 = mB^k = 623$

So send $(719, 623)$.

4.b)

$a = 299$. $A = g^a = 34$.

$c_1 = 661, c_2 = 1325$.

$$\begin{aligned} m &= c_2 c_1^{-299} \\ &= 1325 \cdot 661^{-299} \\ &= 1325 \cdot \left(661^{-1}\right)^{299} \\ &= 1325 \cdot 794 \\ &= 332 \bmod 1373 \end{aligned} \tag{14}$$

4.c)

$B = 893 = g^b \Longrightarrow b = 219$.

$c_1 = 693, c_2 = 793$.

$693 = g^k \Longrightarrow k = 932$.

$$\begin{aligned} 793 &= \left(g^b\right)^k m \\ 792 &= \left(2^{219}\right)^{932} m \\ \Longrightarrow m &= 365 \end{aligned} \tag{15}$$

5)

p, g, A public.

$c_{i,1}$ will be the same for all i so Eve can see that k has not changed.

$$\begin{aligned} c_{i,2} \cdot c_{j,2}^{-1} &= m_i m_j^{-1} \left(g^{ak}\right) \left(g^{ak}\right)^{-1} \\ &= m_i m_j^{-1} \end{aligned} \tag{16}$$

Taking the inverse of $c_{j,2}$ is an *easy* computation!

To decrypt all messages m_i for $2 \leq i \leq n$, Eve does the following.

She can find m_1 and knows $m_1 g^{ak}$. So she easily finds m_1^{-1} to compute $m_1 g^{ak} m_1^{-1} = g^{ak}$. Then she inverts this to get g^{-ak}.

She can use g^{-ak} to find m_i because $c_{i,2} = m_i g^{ak}$, and all k are the same regardless of i. She just does $c_{i,2} g^{-ak} = m_i$.

6)

If Eve has a DHP oracle, show she can break EP.

Goal: use DHP oracle to solve $m = c_2 c_1^{-a} = m(g^a)^k \left(g^k\right)^{-a}$ given $g^a, g^k, m(g^a)^k$.

We can use DHP to compute g^{ak} and then invert using easy operations. So we have g^{-ak}. Then we can multiply this by c_2 to get m.

$$c_2 \cdot g^{-ak} = m g^{ak} g^{-ak} = m \tag{17}$$

7)

7.a)

$$\begin{aligned} u &= m^a \\ v &= u^b = m^{ab} \\ w &= v^a = m^{aba'} \\ m &= w^{b'} = m^{aa'bb'} \end{aligned} \tag{18}$$

We can see that $aa' = 1 \bmod p - 1$ and $bb' = 1 \bmod p - 1$. So $a' = a^{-1}$ and $b' = b^{-1}$ in $\mathbb{Z}/(p-1)\mathbb{Z}$.

If we start with $m = m^{aa'bb'} \bmod p$ and then take the $\log_m$ of both sides, we get $1 = aa'bb' \bmod p - 1$, so it makes sense that a' is the inverse of a mod $p - 1$ and same with b' and b.

So the general version of this system involves Alice picking a message m and private key a (along with $a' = a^{-1} \bmod p - 1$). Then Bob picks private key b (along with $b' = b^{-1} \bmod p - 1$). Using the scheme described in the problem set, we can get m from Alice to Bob without anyone else knowing it. And above we have shown that this will work in general due to how the discrete log works (bring it from mod p to mod $p - 1$).

7.b)

Show if Eve can solve DLP she can solve this system.

Eve knows u, v, w. She can use the fact that $v = u^b$ to find b. Similarly, she can use $w = v^{a'}$ to find a'. Then she can find b' and a using the inverse mod $p - 1$. Once she knows a, a', b, b' she can break this system and solve for m (by exponentiating the public terms, like doing $u^{aa'bb'} = m$).

7.c)

If Eve has a DHP oracle, then she does not necessarily have the ability to solve DLP. Hence she cannot necessarily solve for m.

Given $g^a \bmod p$ and $g^b \bmod p$, Eve can solve for $g^{ab} \bmod p$ because she has an DHP oracle. But in this problem, we want to solve for the value in the exponent, not multiply the exponents of two values. In this system, we continually multiply more values in the exponent, so combining exponents will never allow to find the inverse of the value in the exponent.

For example, given $v = m^{ab}$ and $u = m^a$, we can compute m^{aab}, but that does not get us closer to inverting the values of the exponent to solve for m.